(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04L 12/66

(11) 공개번호 특2002-0079979
(43) 공개일자 2002년10월21일

(21) 출원번호 10-2002-7011455
(22) 출원일자 2002년08월31일
번역문제출일자 2002년08월31일
(86) 국제출원번호 PCT/US2001/06257
(87) 국제공개번호 WO 2001/67258
(86) 국제출원출원일자 2001년02월27일
(87) 국제공개일자 2001년09월13일
(81) 지정국 국내특허 : 아랍에미리트 안티구아바부다 알바니아 아르메니아 오스트리아 오스트레일리아 아제르바이잔 보스니아-헤르체고비나 바베이도스 불가리아 브라질 벨라루스 캐나다 스위스 중국 코스타리카 쿠바 체코 독일 덴마크 도미니카연방 알제리 에스토니아 스페인 핀랜드 영국 그레나다 그루지야 가나 감비아 크로아티아 헝가리 인도네시아 이스라엘 인도 아이슬란드 일본 케냐 키르기즈 북한 대한민국 카자흐스탄 세인트루시아 스리랑카 라이베리아 레소토 리투아니아 룩셈부르크 라트비아 모로코 몰도바 마다가스카르 마케도니아 몽고 말라위 멕시코 모잠비크 노르웨이 뉴질랜드 폴란드 포르투칼 루마니아 러시아 수단 스웨덴 싱가포르 슬로베니아 슬로바키아 시에라리온 타지키스탄 투르크메니스탄 터어키 트리니다드토바고 탄자니아 우크라이나 우간다 우즈베키스탄 베트남 유고슬라비아 남아프리카 짐바브웨 벨리즈 AP ARIPO특허 : 가나 감비아 케냐 레소토 말라위 모잠비크 수단 시에라리온 스와질랜드 탄자니아 우간다 짐바브웨

EA 유라시아특허 : 아르메니아 아제르바이잔 벨라루스 키르기즈 카자흐스탄 몰도바 러시아 타지키스탄 투르크메니스탄

EP 유럽특허 : 오스트리아 벨기에 스위스 사이프러스 독일 덴마크 스페인 핀랜드 프랑스 영국 그리스 아일랜드 이탈리아 룩셈부르크 모나코 네덜란드 포르투칼 스웨덴 터어키

OA OAPI특허 : 부르키나파소 베넹 중앙아프리카 콩고 코트디브와르 카메룬 가봉 기네 기네비쏘 말리 모리타니 니제르 세네갈 차드 토고

(30) 우선권주장 09/518,399 2000년03월03일 미국(US)
(71) 출원인 넥스랜드 인코퍼레이티드
미국 플로리다 33131 마이애미 브리켈 애비뉴 1101 노쓰타워 2층
(72) 발명자 술탄이스라엘다니엘
프랑스폐-75013파리뤼까일로9
(74) 대리인 정진상, 박종혁, 이기석

심사청구 : 없음

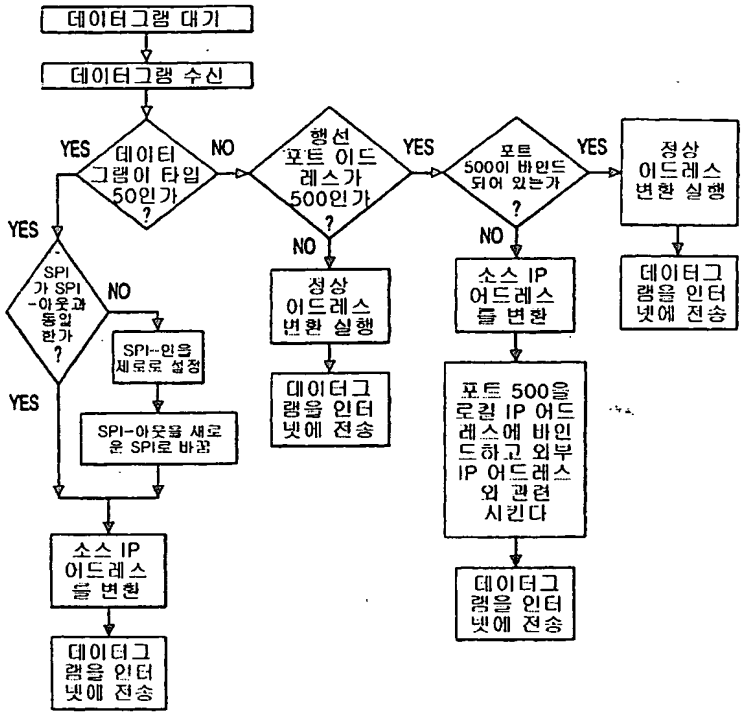
(54) 로컬 IP 어드레스 및 변환불능 포트 어드레스를사용하는 구내 통신망에 대한 네트워크 어드레스 변환게이트웨이

요약

네트워크 어드레스 변환 게이트웨이(20)는 로컬 IP 어드레스를 사용하는 구내 통신망(10)으로부터 외부 네트워크(30)으로 이동하는 IP 데이터그램에 대한 정상 네트워크 변환을 제공하지만, IPSec 프로토콜 모델의 일부인 ISAKMP '핸드셰이킹' 프로토콜과 같이, 특정 프로토콜에 대하여 포트가 예약될 때 소스 서비스 어드레스(포트) 변환을 중지한다. ISAKMP 교환은 소스 및 타겟 컴퓨터 모두가 동일한 서비스 어드레스(포트)를 사용할 것을 요구한다. 소스 서비스 어드레스(포트)를 변환하지 않는 네트워크 인터페이스를 제공함으로써, 이러한 게이트웨이는 로컬 IP 어드레스와 인터넷상의 서버 사이의 IPSec 프로토콜을 사용하여 안전하고, 암호화된 전송의 초기화 및 유지를 가능하게 한다.

대표도

LAN으로부터의 데이터그램에 대한 판정 트리



색인어

네트워크 어드레스 변환 게이트웨이, 로컬 IP 어드레스, 외부 네트워크, 인터넷, 서버, LAN, 소스 서비스 어드레스

명세서

기술분야

TCP/IP를 사용하는 가상 사설망(VPN)은 통신 매체로서 인터넷을 사용하여, 리모트 컴퓨팅 사이트 사이의 안전한 고속 통신을 가능하게 한다. 인터넷을 가로지르는 사이트 사이를 통과하는 정보는 다양한 보안책에 의해 원치않는 도청 또는 악의의 해커에 의해 간섭되는 것으로부터 보호될 수 있다. 효과적인 보안책은 최소한 임의의 또는 모두의 다음의 보호, 즉 전송 동안의 데이터의 부주의하거나 부당한 수정에 대한 데이터 보전; 안티-리피트 방법에 의한 서비스거부공격의 방지; 소스 인증; 전송 동안의 다른 헤더 정보 및 소스 어드레스의 신뢰도; 및 원치않는 간섭에 대한 패킷 페이로드 보호를 보장하는 기능을 포함해야 한다. 인터넷 보안을 제공하는 하나의 스탠더드 모델은 인터넷 프로토콜 보안 슈트, IPSec이다. IPSec는 자체 인터넷에 연결된 사설 LANs(구내 통신망)에 연결되거나 인터넷에 연결된 디바이스 사이에서 안전한 통신을 제공하기 위해 TCP/IP 통신 프로토콜과 함께 동작한다.

배경기술

TCP/IP(전송 제어 프로토콜/인터넷 프로토콜) 프로토콜 슈트는 네트워크상의 각각의 디바이스를 식별하기 위해 IP 어드레스를 사용한다. 글로벌 IP 어드레스는 유일한 인터넷상의 디바이스를 식별한다. 이러한 디바이스는 컴퓨터, 프린터, 루터, 스위치, 게이트웨이 또는 다른 네트워크 디바이스일 수 있다. 글로벌 IP 어드레스를 갖는 디바이스는 인터넷상의 소스 또는 행선지로서 직접 참조될 수 있다. 하지만, TCP/IP 통신 프로토콜은 인터넷에 배타적으로 제한되지 않고 사설 LANs에서도 물론 사용될 수 있다. TCP/IP를 자주 사용하는 LANs는 네트워크에 대한 '로컬' IP 어드레스를 사용한다. 사설 LAN 상의 어떤 2개의 디바이스도 동일한 로컬 IP 어드레스를 공유할 수 없지만, 사설 LANs는 인터넷으로부터 격리되어 LAN상의 로컬 디바이스는 인터넷으로부터 보이지 않을 수 있다. 따라서, 로컬 디바이스에 대한 IP 어드레스는 '전세계적으로' 유일할 필요가 없다. 로컬 IP 어드레스를 사용하는 LAN은 LAN과 인터넷사이의 메시지를 필터링하거나 루팅할 수 있는 디바이스인 게이트웨이를 통하여 인터넷에 연결될 것이다. 게이트웨이가 인터넷에 직접 부착되어 있기 때문에, 게이트웨이는 인터넷을 가로지르는 통신에 대한 전세계적으로 유일한 IP 어드레스를 가져야 한다. 그러나, LAN이 인터넷으로부터 직접 보이지 않기 때문에, LAN상의 로컬 머신은 전세계적으로 유일한 IP 어드레스를 필요로 하지 않는다.

TCP/IP는 인터넷상에 사용되는 통신 프로토콜이다. TCP/IP를 사용하여 통신되는 정보는 '데이터그램'내

에 포함된다. 데이터그램은 하나 이상의 헤더가 부가된 정보의 이산적인 '패킷'으로 구성되어 있다. 헤더는 패킷을 그 의도된 행선지로 보내고 전송 동안 패킷의 적합한 처리를 보장하기 위해 TCP/IP에 의해 필요한 정보를 포함한다. 각각의 데이터그램은 개별적으로 어드레스가능하고, 접속식 TCP 데이터그램 또는 '커넥션레스형' UDP(사용자 데이터그램 프로토콜) 데이터그램일 수 있다. 각각의 UDP 데이터그램은 IP 헤더 및 UDP 헤더를 포함한다. IP 헤더는 적어도 '소스' IP 어드레스 및 '행선' IP 어드레스를 포함하고, UDP 헤더는 소스 및 행선 서비스 어드레스(포트 어드레스, 넘버로 주어진다)를 포함한다. IPv4, IP 어드레스는 길이가 32 비트이고, 이제는 친숙한 xxx.xxx.xxx.xxx 포맷과 관련되어 있다. 이러한 포맷에서, 각각의 3-디짓 세드먼트는 0과 255 사이의 넘버를 나타내는 2진법 옥텟이다. 완전한 IP 어드레스는 로컬 어드레스의 어드레스 또는 네트워크 세그먼트를 네트워크상의 '노드'(디바이스)의 어드레스와 조합한다. 네트워크 또는 네트워크 세그먼트의 어드레스는 IP 어드레스의 제1 3, 6, 또는 9 디짓을 포함할 수 있다. 네트워크 또는 네트워크 세그먼트상의 디바이스는 네트워크 또는 네트워크 어드레스에서 사용되지 않는 잔여 디짓으로 구성된 노드 어드레스에 의해 식별된다.

UDP 헤더내에 포함된 소스 및 행선 서비스 어드레스는 전송 또는 수신 디바이스에 액티브한 의도된 프로세스로 패킷을 지향시키도록 하기 위해 사용되는, '포트' 또는 '소켓'으로 다양하게 알려진 16비트 넘버이다. 여기에 사용된 용어 '포트' 또는 '포트 어드레스'는 UDP 헤더내의 서비스 어드레스 필드를 가리킨다. 이론적으로 16비트 수의 어드레스가 존재하지만, 약속에 의해 많은 포트 어드레스가 달성된 프로세스에 대해 예약되어 있다. 따라서, 예를 들어, 포트 80은 HTTP에 대하여 예약되어 있고, 포트 20 및 21은 FTP에 대하여 예약되어 있다. 포트 어드레스를 사용함으로써, 하나 이상의 프로세스를 실행하는 로컬 머신에 도착한 데이터는 의도된 프로세스로 지향된다. 로컬 호스트에서 실행되는 프로세스가 예약된 프로세스중 하나가 아닌 경우에, 로컬 호스트는 '소스' 프로세스를 식별하기 위해 예약되지 않은 포트 넘버의 풀로부터 임의의 포트 넘버를 선택할 수 있다. '행선' 필드내의 포트 넘버를 참조하는 응답 패킷은 상기 프로세스로 전송된다.

지난 10년간 인터넷 사용의 폭발적인 증가 및 인터넷의 예측되는 미래의 성장과 함께, 전세계적으로 유일한 IP 어드레스는 진귀한 리소스가 되었다. 또한, 사설 LANs를 유지하는 많은 비지니스는 각각의 컴퓨터 및 LAN 상의 디바이스가 유일한 글로벌 IP 어드레스를 가질 필요가 거의 없거나 전혀 없다. 그러한 많은 비지니스는 임의의 이벤트에 그들의 컴퓨터의 IP 어드레스의 신뢰도를 유지하는 것이 바람직하다. 각각의 로컬 디바이스에 유일한 글로벌 IP 어드레스를 줌으로써 제한된 글로벌 리소스를 낭비하기 보다는 오히려 많은 사설 LANs는 LAN상의 디바이스에 대한 로컬 IP 어드레스를 사용한다. 인터넷에 접속하기 위해, 그러한 LANs는 인터넷으로부터 LAN을 분리하는 게이트웨이에 의해 인터넷상에 사용되도록 하나의 전세계적으로 유일한 어드레스를 사용한다.

네트워크 어드레스 변환(NAT) 기술을 사용함으로써, 인터넷으로부터 LAN을 분리하는 게이트웨이 디바이스는 로컬 IP 어드레스를 가진 머신이 게이트웨이의 유일한 글로벌 어드레스를 통해 인터넷에 액세스할 수 있도록 하면서 방화벽으로서 보안성을 제공한다. LAN상의 디바이스는 정적 로컬 IP 어드레스를 가질 수 있거나 로그 온에서 상기 디바이스에 동적 할당된 로컬 IP 어드레스를 가질 수 있다. 게이트웨이는 LAN상의 각각의 디바이스에 대하여 로컬 IP 어드레스를 갖는 변환 테이블을 유지한다. 로컬 머신으로부터 전송되고 인터넷이 행선지인 UDP 패킷은 IP의 소스 필드 및 UDP 헤더에서 식별되는 로컬 IP 어드레스 및 포트 어드레스를 각각 갖는다. 게이트웨이는 로컬 머신으로부터 패킷을 수신하고 IP 및 UDP 헤더의 소스 필드내로 게이트웨이의 전세계적으로 유일한 IP 어드레스 및 (사용되지 않고 예약되지 않은 포트 어드레스의 풀로부터 취해진) 새로운 포트 어드레스를 대입한다. 다음으로, 게이트웨이는 CRC(순환 중복 검사)를 업데이트하고 임의의 다른 필요한 변화를 만들어 데이터 보전을 보장하고, 그후에 패킷을 인터넷에 전송한다. 프로세스의 일부로서, 게이트웨이는 로컬 머신의 IP 어드레스를 상기 머신에 의해 처음 보고된 소스 포트 어드레스, 인터넷에 바인드된 패킷에 할당된 새로운 소스 포트 어드레스, 그리고 행선 IP 어드레스와 상호 참조하기 위해 게이트웨이의 내부 변환 테이블을 업데이트한다. 인터넷으로부터 응답을 수신할 때에, 게이트웨이는 패킷 헤더내의 자체 IP 어드레스를 인식하고 입중계 패킷의 행선 포트 어드레스를 검사한다. 게이트웨이가 그 내부 테이블에서 행선 포트를 발견하면, 게이트웨이는 상호 참조된 로컬 머신의 IP 어드레스 및 본래의 포트 어드레스를 패킷의 행선 필드내에 대입하고, CRC 및 임의의 다른 필요한 파라미터를 업데이트하고, 그후에 패킷이 로컬 머신에 의해 수신되어 적당한 프로세스로 지향되는 패킷을 LAN에 디스패치한다. 이러한 방식으로, 로컬 IP 어드레스만을 갖는 LAN 상의 다수의 컴퓨터는 하나의 전세계적으로 유일한 IP 어드레스를 통해 인터넷과 통신할 수 있다.

NAT 게이트웨이가 인터넷으로부터 LAN의 직접 액세스에 대한 방화벽 보안을 제공하지만, NAT 게이트웨이는 인터넷상의 전송 동안 LAN으로 의도된 패킷의 방수 또는 수정에 대한 보안을 제공하지 않고, LAN내에서 발생된 문제로부터의 '신뢰성'을 보장하지는 않는다. 따라서, IPSec에 의해 제공된 보안은 인터넷과 인터페이스하는 동안 보안을 유지해야 하는 LANs에 대해 필요한 보호이다.

IPSec의 일반적인 실현은 적어도 하나의 메인 컴퓨팅 사이트 및 하나 이상의 리모트 LANs으로 구성된 VPNs에 대한 보안을 제공하는 것이다. 메인 사이트 및 리모트 LANs는 사이트 사이의 통신을 위해 상당하게 보다 비싼 사설 임대 라인 대신에 고속 매체를 사용하여 인터넷을 가로질러 연결되어 있다. 그러나, 전송 매체로서 인터넷을 사용하는 단점은 인터넷이 본래 불안전하고 해커에 의해 메시지의 스누핑, 검출, '속임수(spoofing)' 또는 궁극적인 절도, 수정 또는 분산에 대하여 본래의 보호가 거의 없거나 전혀 없다는 것이다. 따라서, 안전한 데이터 전송이 요구되는 포괄적인 보안 대책이 필요하다. IPSec 프로토콜은 데이터 및 데이터 보전의 인증을 보장하기 위해 보안 방법을 구현한다.

IPSec 프로토콜 슈트는 다층 OSI(개방 시스템간 상호접속) 네트워크 참조 모델의 네트워크층에서 보안을 구현한다. 슈트는 인터넷을 통하여 정보를 전달하는 UDP 데이터그램의 보안을 보장하기 위해 서로 연결되어 사용되는 다수의 별개의 프로토콜을 포함한다. IPSec 컴플라이언트 시스템의 기본 구조는 RFC2401, 'Security Architecture for the Internet Protocol,' S. Kent and R. Atkinson(November 1998)에 설명되어 있다. AH(인증 헤더) 프로토콜은 데이터 보전, 소스 인증을 보장하고, 서비스거부공격을 막기 위하여 '안티-리피트' 방법을 포함한다. ESP(Encapsulation Security Payload) 프로토콜은 AH와 유사한 보호를 제공하지만, 페이로드 암호화의 추가 특징이 부가되어 있다. AH 및 ESP 헤더 모두는 시큐어리티 파라미터 인덱스(SPI)에 대한 필드를 갖는다. SPI는 데이터그램에 대하여 시큐어리티 오소시에이션(SA)을 식

별하기 위하여 사용되는 32 비트 의사난수값이다. 이러한 프로토콜에 대한 추가 정보는 RFC1826, 'IP Authentication Header,' by R.Atkinson (August 1995), and RFC2406, 'IP Encapsulating Security Payload(ESP),' S.Kent R.Atkinson(November 1998)에서 발견할 수 있다. ISAKMP/Oakley (인터넷 시큐어리티 어소시에이션 및 키 관리 프로토콜, 또한 보통 인터넷 키 익스체인지-IKE로 불린다)는 2개의 호스트 사이트 사이의 보안 세션에 대한 파라미터를 달성하는 핸드셰이킹 프로토콜이고, 보안 세션을 구현하고 암호화된 데이터의 전송을 허용하기 위해 사용되는 키잉 및 시큐어리티 정보의 교환에 대해 제공한다. ISAKMP/Oakley 프로토콜(이후로는 단순히 ISAKMP로 부른다)은 인증이 달성될 수 있고 데이터 암호화에 대한 보안 키가 발생될 수 있는 초기화 데이터를 양쪽 머신 모두에 제공하기 위해 암호화된 메시지의 초기 교환을 포함한다. 이러한 프로세스의 설명은 RFC2409, 'The Internet Key Exchange,' D. Harkins and D. Carrel(November, 1998)에서 발견될 수 있다. 일단 호스트 사이에 시큐어리티 어소시에이션(SAs)를 충분히 달성하는 시큐어리티 파라미터가 교환되었다면, 모든 후속 전송은 암호화되고 동의에 기초한 프로토콜에 따라 완전히 인증된다. 이 포인트에서 ISAKMP 프로토콜은 종료한다. 후속 어드레싱은 각각의 머신에 대한 IP 어드레스 및 상기 세션에 대한 머신의 SPI에 기초한다. SPI는 세션 동안 각각의 머신에 대하여 유일하다. 사설 LAN 에 대한 게이트웨이는 로컬 머신의 IP 어드레스에 상호참조되는 값내의 'SPI-인' 및 'SPI-아웃'이 로컬 머신과 통신하는 인터넷상의 머신의 IP 어드레스에 상호참조되는 내부 테이블을 유지한다. 각각의 머신에 대한 SPI는 ISAKMP 전송 동안 교환되는 정보로부터 계산되고 UDP 패킷에 부착되는 AH 또는 ESP 헤더에 전달된다. IPSec 프로토콜이 다양한 환경에서 보안을 제공하도록 네스팅될 수 있기 때문에, 단일 데이터그램은 AH 및 ESP 헤더 모두를 포함할 수 있고, 임의의 헤더 정보를 암호화할 수 있다.

상기 시큐어리티 프로토콜의 각각은 패킷에 새로운 헤더 정보를 놓고, 사용중인 프로토콜에 합치하기 위해 패킷내의 특정 필드를 수정하며, 특정 경우에, 페이로드 및 다른 패킷 헤더의 모든 또는 일부를 암호화함으로써 UDP 패킷을 수정한다. 따라서, IPSec하에서, UDP 데이터그램은 신뢰받지 못한 네트워크를 가로질러 전송되기 위해 '안전한' 도메인을 떠날 때, 보통 IP 헤더, AH 또는 ESP 헤더 (또는 모두), 및 캡슐화된 페이로드로 구성된다. 헤더 정보는 행선 어드레스, SPI 및 충분한 SA 정보를 포함하여 데이터그램이 그 행선지에 도달하고 행선지 호스트에 인증될 수 있도록 보장한다. 페이로드를 캡슐화하면 페이로드내에 포함된 정보가 원치않는 도청자 및 해커에게 거부되는 것을 보장할 수 있다. 데이터그램에 대한 초기 행선 호스트는 루터, 게이트웨이, 또는 LAN과 인터넷 사이의 방화벽일 수 있다. LAN과 인터넷 사이의 경계상의 디바이스에 도착할 때, 데이터그램은 오픈, 검사 또는 전체 또는 부분적으로 암호화될 수 있고, 추가 어드레스 정보에 대하여 분석되어 LAN 상의 로컬 IP 어드레스에 루팅될 수 있다.

IPSec에서 사용되는 ISAKMP 핸드셰이킹 프로토콜은 사이에 보안 세션을 달성하도록 의도된 호스트 모두가 초기 메시지 교환에 대하여 프로세스-특정 포트 어드레스(포트 500)를 사용할 것을 요구한다. 이러한 이유에서, 포트 500은 ISAKMP 프로토콜에 독점적으로 사용되도록 할당되었다. 관습상, ISAMP 프로토콜을 사용함으로써 보안 통신 파라미터의 협상을 시도하는 컴퓨터는 각각의 컴퓨터의 포트 500을 통해서 제한적으로 통신해야 한다. 즉, 임의의 컴퓨터로부터의 ISAKMP 메시지는 포트 500을 소스 및 행선 포트 어드레스 모두로서 식별해야 한다. 포트 500이 소스 및 행선지 모두로서 명세화되지 않은 패킷을 임의의 컴퓨터가 수신한다면, 패킷은 버려지게 된다.

이러한 프로토콜이 2개의 호스트가 서로 통신하도록 보장하지만, 로컬 IP 어드레스 및 NAT 게이트웨이를 사용하는 LAN상에 하나의 호스트가 위치될 때 작동불능이 될 수 있다. 예를 들어, NAT 게이트웨이에 의해 보호되는 리모트 LAN 상의 로컬 IP 어드레스를 갖는 호스트 A는 메인 오피스 컴퓨팅 사이트에 위치된 호스트 B와 보안 세션을 달성하기를 원한다. 호스트 A는 암호화된 UDP 데이터그램을 호스트 B에 전송하고, '행선 어드레스'를 호스트 B의 IP 어드레스로서 그리고, 행선 포트 어드레스를 '포트 500'으로서 줌으로써 프로토콜을 초기화한다. 그러나, 데이터그램이 LAN을 인터넷에 접속하는 NAT 게이트웨이에 도달할 때, 게이트웨이는 행선 포트 어드레스를 보조 포트 넘버로 변환한다. 호스트 B에 데이터그램이 도착할 때, ISAKMP 프로토콜은 인식되고, 호스트 B는 응답하지 않는다. 컴퓨터는 보안 세션을 달성하는데 실패한다. 이러한 문제로 인해, 리모트 LAN 상의 각각의 컴퓨터가 글로벌 IP 어드레스보다 로컬 IP 어드레스를 사용하는 NAT 게이트웨이를 사용하여 VPN을 달성하기 위해 ISAKMP 프로토콜이 사용될 수 없다고 생각되어왔다.

따라서, 전송 매체로서 인터넷을 사용하여, 논-글로벌 IP 어드레스를 갖는 컴퓨터 및 호스트 컴퓨터 사이의 키 교환 및 ISAKMP 프로토콜 인증의 사용을 허용하는 게이트웨이를 제공하는 것이 본 발명의 목적이다.

또한, 본 발명의 목적은 로컬 IP 어드레스를 사용하는 사설 LAN 상의 임의의 수의 컴퓨터가 ISAKMP 프로토콜을 사용하여 인터넷을 통하여 메시지를 초기화하거나 수신할 수 있도록 하는 게이트웨이를 제공하는 것이다.

본 발명의 또 다른 목적은 보안 통신을 초기화하기 위해 ISAKMP 프로토콜을 사용하여, 인터넷상의 2개 이상의 LAN 사이트 사이에 가상 사설 네트워킹을 사용하는 방법을 제공하는 것이다.

본 발명의 상기 방법 및 다른 방법은 아래의 설명을 통해 명백해질 것이다.

발명의 상세한 설명

발명의 개시

본 발명에 따라, NAT 게이트웨이를 통해 인터넷과 같은 외부 네트워크에 연결된 리모트 LAN 상의 로컬 IP 어드레스를 사용하는 컴퓨터는 IPSec하에 보안 세션을 지원하는 SAs를 달성하고 키를 교환하기 위해 ISAKMP 프로토콜을 사용한다. 논-ISAKMP 트랙픽에 대하여, 게이트웨이는 어드레스 변환을 정상적으로 실행한다. 그러나, LAN상의 머신이 ISAKMP 프로토콜 메시지를 발생할 때마다, 게이트웨이는 포트 500의 포트 어드레스를 포함하는 데이터그램을 식별한다. 그러한 데이터그램을 만났을 때, 게이트웨이는 소스 IP 어드레스를 변환하지만, 소스 포트 어드레스를 변환하지 않고, 소스 포트 어드레스를 포트 500에 놓고, 소스 및 행선 포트 어드레스 모두로서 지정된 포트 500으로 인터넷에 패킷을 디스패치한다. 게이트웨이

는 또한 로컬 IP 어드레스에 포트 500을 '바인드'하기 위해 게이트웨이의 내부 테이블을 업데이트하고 소정 시간동안 행선지 머신의 외부 IP 어드레스와 상기 바인딩을 관련시킨다. 유효한 응답이 소정의 시간내에 수신되지 않았다면, 포트 500과 로컬 IP 어드레스 사이의 '바인딩'은 해제된다. 이러한 특징은 예를 들어, 부정확한 행선 IP 어드레스에 ISAKMP 프로토콜 전송이 초기화된 상황에서와 같이, 포트 500이 무제한으로 타이 업되지 않도록 보장하기 위해 필요하다. 이러한 컨디션에서, 게이트웨이는 유효한 응답을 절대 수신하지 않는다. 유효한 응답이 수신되지 않은 기간후에 포트 500을 해제하는 타이머가 존재하지 않는다면, 포트는 게이트웨이가 리셋될 때까지 로컬 IP 어드레스에 바인드된 상태로 남아 있게 된다. 대부분의 컨디션에 대하여, 2초의 기간은 유효한 응답을 기다리는 동안 포트 500과 로컬 IP 어드레스 사이의 바인딩을 유지하기 위해 충분한 시간이어야 한다.

포트 500이 로컬 IP 어드레스에 바인드되어 있는 동안에, 게이트웨이는 유효한 응답을 기다리는 동안 포트 500 포트 어드레스를 갖지 않는 데이터그램의 정상 데이터그램 프로세싱을 계속한다. 유효한 응답은 포트 500과 관련된 외부 IP 어드레스오 동일한 소스 IP 어드레스를 갖는 데이터그램이고, 포트 500으로서 소스 및 행선 포트 어드레스 모두를 갖는다. 유효한 응답을 기다리는 동안, 게이트웨이는 포트 500 소스 및 행선 포트 어드레스를 갖지만, 적합한 소스 IP 어드레스를 갖지 않는 외부 네트워크로부터 다른 UDP 데이터그램을 무시한다. 또한, 포트 500이 로컬 IP 어드레스에 바인드되어 있는 동안, 포트 500의 소스 행선 포트 어드레스를 갖는 LAN으로부터 수신된 데이터그램은 외부 네트워크에 전송되기 전에 보조, 사용되지 않는 포트 어드레스로 포트 500 소스 포트 어드레스가 변환되는 '정상' 어드레스 변환 과정을 거치게 된다. 그러한 데이터그램이 포트 500의 소스 및 행선 포트 어드레스 모두를 가지지 않기 때문에, 이 데이터그램은 유효한 ISAKMP 데이터그램이 아니고, 상기 데이터그램의 IP 행선지에 도달할 때 무시된다. 포트 500을 로컬 IP 어드레스에 바인딩하는 기간이 게이트웨이에 수신된 유효한 데이터그램 없이 종료되어야 한다면, 바인딩은 해제되고, 포트 500은 포트 500 소스 및 행선 포트 어드레스를 갖는 다음 데이터그램에 의해 사용되기 유용하게 된다.

포트 500가 바인드되어 있는 동안에, 정확한 소스 IP 어드레스 및 포트 500의 소스 및 행선 포트 어드레스를 갖는 유효한 응답 데이터그램을 수신할 때, 게이트웨이는 로컬 머신의 IP 어드레스를 데이터그램 헤더의 행선 IP 어드레스 필드에 대입함으로써 데이터그램을 처리한 후에, 로컬 머신에 전달하기 위해 LAN을 통하여 데이터그램을 전송한다. 데이터그램이 게이트웨이를 떠날 때, 게이트웨이는 로컬 IP 어드레스와 포트 500 사이의 바인딩을 해제하고, 정상 데이터그램 프로세싱을 계속한다.

포트 500의 적합한 소스 IP 어드레스 및 포트 어드레스를 갖는 응답이 외부 네트워크로부터 수신되지 않는다면, 게이트웨이는 소정의 단시간후에 타임 아웃된다. 게이트웨이가 유효한 응답이 수신되기 전에 타임 아웃되어야 한다면, ISAKMP 메시지 교환은 완료될 수 없고 다시 초기화되어야 한다.

일단, ISAMP 프로토콜이 완료되었고 암호화된 보안 세션이 진행중이라면, 게이트웨이는 입중계 및 출중계 데이터그램의 ESP 헤더내의 SPI를 참조함으로써 로컬 어드레스 변환을 실행한다. 게이트웨이는 또한 각각의 패킷 타입(ESP 패킷에 대한 타입 50)이 게이트웨이를 통과하는 데이터그램에 대하여 정확할 것을 보장한다. 종종, VPN을 통한 보안 세션은 인터럽트되거나 새로운 세션이 시작된다. 이것의 게이트웨이의 제1 표시는 IP 어드레스가 인식되지만 행선지와 관련된 SPI가 게이트웨이의 내부 테이블내에 나타나지 않는 타입 50 데이터그램을 수신하는 것이다. 이것이 발생할 때, 게이트웨이는 새로운 SPI를 사용하여 행선 IP 어드레스에 데이터그램을 디스패치하고, 게이트웨이의 테이블내의 행선 SPI 값(전송 방향에 의존하는 SPI-인 또는 SPI-아웃)을 새로운 값으로, 그리고 소스의 SPI 값을 제로로 설정한다. 응답을 전송부로 수신할 때, 게이트웨이는 SPI 필드 테이블내의 제로를 행선 IP 어드레스에 대한 새로운 SPI로 대체한다.

본 발명의 게이트웨이가 메시지를 암호화하거나 해독하지 않고 단순히 (암호화되거나 해독될 수 있는) 페이로드를 수신 머신에서의 처리를 위해 LAN 또는 인터넷으로 통과시키기 때문에, 게이트웨이는 강력한 처리 기능을 필요로 하지 않고 셋업 및 유지의 비용 및 단순성이 문제가 되는 사설 LANs용으로 사용될 수 있다.

도면의 간단한 설명

도 1은 인터넷일 수 있는 외부 네트워크를 통하여 메인 컴퓨팅 사이트와 로컬 IP 어드레스를 사용하고 NAT 게이트웨이를 통하여 외부 네트워크에 연결된 리모트 LAN이 네트워크되는 가상 사설망을 도시한 도면,

도 2는 LAN으로부터 인터넷으로 전송하기 위해 수신된 UDP 데이터그램을 처리하도록 본 발명의 게이트웨이에 의해 사용되는 판정 차트를 도시한 도면,

도 3은 인터넷으로부터 LAN 상의 디바이스에 전달하기 위해 수신된 UDP 데이터 그램을 처리하기 위해 본 발명의 게이트웨이에 의해 사용되는 스텝의 판정 차트를 도시한 도면,

도 4는 도 5, 도 6, 도 7에 도시된 차트를 따르는데 있어서 참조하기 위해 제공된, LAN(L-1 내지 L-3) 상의 로컬 머신의 IP 어드레스, 게이트웨이의 내부 및 외부 P 어드레스, 및 외부 네트워크상의 외부 디바이스('타겟' T-1 내지 T-3)의 IP 어드레스를 포함하는 표,

도 5a -5c 는 암호화된 데이터그램을 인증하기 위해 사용된 SPIs(시큐어리티 파라미터 인덱스)와 함께 외부 디바이스(T-1 내지 T-3)의 외부 IP 어드레스 및 LA(L-1, L-2, . . . L-x)상의 머신의 로컬 IP 어드레스를 상호 참조하는 게이트웨이의 내부 테이블로부터의 대표적인 필드를 도시하는 도면으로서, SPI-아웃은 인터넷상의 디바이스에 대한 게이트웨이를 떠나는 암호화된 데이터그램의 SPI를 나타내고, SPI-인은 LAN 상의 로컬 머신이 행선지인 암호화된 데이터그램의 SPI를 나타내고, 표 a,b,c는 각각은 상이한 시점에서의 소스, 행선지 및 SPI에 대한 헤더 값을 나타낸다. 변화값은 타겟 머신과 함께 로컬 머신 하나에 의한 새로운 세션의 개시를 의미한다.

도 6은 외부 네트워크상의 단일 디바이스 및 단일 로컬 머신 사이에 교환되는 데이터그램 헤더내의 대표적인 필드를 도시하는 도면으로서 헤드값은 본 발명의 게이트웨이에 의해 처리함으로써 수정된다.

도 7은 외부 네트워크 상의 3개의 타겟(T-1 내지 T-3) 머신과 LAN상의 3개의 로컬 머신(L-1 내지 L-3)이 본 발명의 게이트웨이에 의해 처리됨으로써 수정될 때 외부 네트워크 상의 3개의 타겟(T-1 내지 T-3) 머신과 LAN상의 3개의 로컬 머신(L-1 내지 L-3)사이에서 교환되는 데이터그램 헤더내의 대표적인 필드를 도시하는 도면, 및

도 8은 데이터그램 처리 펑션과 타이머 사이를 통과하는 신호의 개략도.

실시예

도 1에 사설 구내 통신망(LAN; 10)이 인터넷(50)상에 위치된 컴퓨팅 사이트(30)에 연결되어 있는 가상 사설망(VPN)이 도시되어 있다. LAN(10)은 로컬 IP 어드레스를 사용하고, 본 발명의 네트워크 주소 변환(NAT) 게이트웨이(20)를 통해 인터넷에 연결되어 있다. 컴퓨팅 사이트(30)는 비즈니스 헤드쿼터, 또는 다국적 기업, 교육기관, 또는 리모트 로케이션으로부터 자주 액세스되는 임의의 다른 사이트에 의해 사용되는 임의의 수의 사설 LANs중 하나일 수 있다. 이러한 사이트는 암호화 및 다른 보안 애플리케이션을 실행할 수 있는 게이트웨이(35) 또는 방화벽을 보통 가질 것이다. 이러한 게이트웨이는 패킷을 오픈하거나 그 콘텐츠를 해독하거나 액세스하고 주소 변환, 루팅, 캡슐화해제 및 데이터 조작 펑션도 역시 실행하는 능력을 갖게 된다. 이러한 디바이스는 ISAKMP 및 다른 IPSec 프로토콜을 지원할 수 있고 패킷을 개방하거나 해독하고 데이터를 조작함으로써 ISAKMP 및 다른 IPSec 프로토콜을 지원하지만, 메인 컴퓨팅 사이트로 VPN을 달성하기 위해 필요한 리모트 LAN 사이트에서 효율적으로 사용되기에는 방대하고, 너무 비싸고 강력하다.

메인 사이트에서의 서버(40)는 VPN 서버 소프트웨어를 실행한다. 리모트 사이트에서의 컴퓨터(15) 각각은 각각의 컴퓨터상에 IPSec 시큐어리티 프로토콜을 구현하는 적합한 VPN 클라이언트 소프트웨어를 실행한다.

LAN(10)상의 컴퓨터(15)는 IP 데이터그램을 컴퓨팅 사이트(30)에서의 서버(40)에 전송함으로써 게이트웨이(20)를 통하여 인터넷 상의 또는 인터넷을 가로지르는 디바이스와 통신한다.

게이트웨이(20)에서 수신된 데이터그램은 도 2 및 도 3에 도시된 판정 차트에 따라 처리된다. 도 2 및 도 3의 순서도가 처리 스텝 및 이 스텝에 대한 시퀀스 모두를 도시하지만, 상기 펑션의 일부를 실행하는 순서는 중요하지 않고 상기 스텝의 일부는 최종 결과에 영향을 주지 않고 순서도에 도시된 것과 다른 순서로 이루어질 수 있다. 예를 들어, 도 2 및 도 3은 데이터그램이 게이트웨이에 의해 수신된 후의 제1 스텝이 데이터그램 타입을 결정하는 것이고, 마지막 스텝이 데이터그램이 게이트웨이를 통과하기 전에 필요한 IP 주소 변환을 실행하는 것이라고 도시한다. 그러나, 일부 실시예는 프로세스내에서 보다 빠른 특정 포인트에 주소 변환의 스텝을 놓을 수 있고, 이것은 프로세스의 결과에 영향을 주지 않는다. IP 주소를 변환하는 순서는 전체 프로세서에 중요하지 않기 때문에, 이러한 변환이 언제 이루어져야 하는지에 대한 결정은 엔지니어링 선택의 문제이다.

도 2에 도시된 바와 같이, LAN으로부터 데이터그램을 수신시, 게이트웨이는 데이터그램이 암호화되었는지를 보기 위해 검사할 것이다. 이것은 게이트웨이가 다루는 데이터그램의 타입을 결정하고 데이터그램이 암호화되었는지를 보기 위해 IP 헤더내의 '넥스트 헤더'를 체크함으로써 이루어진다. 50의 데이터그램 타입(ESP)은 데이터그램이 암호화되었음을 나타내고, 포트 어드레스 정보는 유용하지 않다.

계속해서 도 2의 판정 트리에서, 데이터그램이 암호화되었다면, 게이트웨이는 데이터그램의 SPI를 체크하여 게이트웨이의 내부 테이블의 SPI-아웃 필드내에 나타나는지를 본다. 그러한 테이블로부터의 대표적 필드는 도 5a-도 5c내에 도시되어 있다. 만약 데이터그램의 SPI가 내부 테이블의 SPI-아웃 필드내에서 발견되었다면, 게이트웨이는 데이터그램의 소스 IP 어드레스를 데이터그램의 외부 IP 어드레스가 되도록 수정하고, 외부 디바이스에 전달하기 위해 외부 네트워크에 데이터그램을 전송한다.

데이터그램이 암호화되었지만, SPI가 게이트웨이의 내부 테이블내에 나타나지 않았다면, 도 2의 판정 차트에 따라 게이트웨이는 데이터그램이 새로운 세션을 초기화한다고 여기게 된다. 이러한 경우에, 게이트웨이는 그 내부 테이블의 SPI-인 필드를 제로(0)으로 설정하고 데이터그램으로부터 SPI-아웃을 새로운 SPI로 설정하게 된다. 내부 테이블에 대한 이러한 수정은 도 5a내의 게이트웨이의 내부 테이블의 SPI-아웃 필드내에 나타나지 않는 '새로운' SPI('14662')가 SPI-아웃 필드로 입력된 것으로 도시되어있고 SPI-인은 도 5b내에 제로(0)로 설정되어 있는 도 5a 및 도 5b에 나타나있다. 그다음, 암호화된 데이터그램은 소스 IP 어드레스가 로컬 디바이스의 어드레스로부터 게이트웨이의 외부 IP 어드레스로 변환된 후에 외부 게이트에 전송된다. 이러한 스텝은 도 5b 및 도 5c에 도시되어 있다.

계속 도 2의 판정 차트에서, 데이터그램이 암호화되지 않았다면, 다음으로 게이트웨이는 데이터그램의 행선지 포트 어드레스를 체크하게 된다. 포트 어드레스가 포트 500이외의 다른 것이라면, 게이트웨이는 소트 포트 어드레스를 그 내부 테이블로 입력시켜 (로컬) 소스 IP 어드레스와 상호 참조하고, 그다음, 보조, 사용되지 않는 포트 어드레스를 IP 헤더의 소스 포트 어드레스 필드와 바꾼다. 또한 게이트웨이는 그 내부 테이블내에 새로운 포트 어드레스를 입력시켜 다시 소스 IP 어드레스와 상호 참조시킨다. 포트 어드레스로서 포트 500을 갖지 않는 암호화되지 않은 데이터그램에 대하여 사용되는 이러한 프로세스는 LAN상에서 발생된 데이터그램에 대한 '정상 어드레스 변환'으로 불리게 될 것이다. 이러한 변환은 도 6내의 행 1과 2에 도시되어 있다. 데이터그램은 그다음, 행선 IP 어드레스에 루팅되기 위해 인터넷에 디스패치된다.

다음으로 게이트웨이는 입중계 데이터그램의 소스 및 행선 포트 어드레스가 포트 500인 도 2에서 포트 500이 이미 IP 어드레스에 바인드되었는지를 보기 위해 게이트웨이의 테이블을 체크해야 한다. 포트 500이 프리라면, 게이트웨이는 데이터그램의 (로컬) 소스 IP 어드레스에 포트 500을 '바인드'하고 포트와 (외부) 행선 IP 어드레스 사이에 관련성을 생성하며 내부 타이머를 시작하기 위해 신호를 보낼 것이다. 또한 게이트웨이는 소스 IP 어드레스 필드내의 로컬 IP 어드레스 대신 게이트웨이의 외부 IP 어드레스를 대입함으로써 데이터그램을 처리한다. 그러나, 게이트웨이는 소스 포트 어드레스를 변환하지는 않는다. 소스 포트 어드레스의 '정상' 변환을 중지시킴으로써, 게이트웨이는 타겟 머신이 데이터그램을 ISAKM 데

이터그램으로 인식할 수 있도록 보장한다. 이러한 스텝은 또한 도 6의 행 5,6에 도시되어 있다.

도 2에서, LAN으로부터의 입중계 데이터그램이 포트 500의 행선 포트 어드레스 및 소스를 갖지만, 포트 500이 이미 임의의 다른 로컬 IP 어드레스에 바인드되었다면, 게이트웨이는 처리를 위해 메시지에 대한 포트 500을 바인드할 수 없다. 이러한 경우에, 게이트웨이는 그것이 ISAKMP 데이터그램이 아닌 것처럼 데이터그램을 '정상적으로' 처리한다. 즉, 게이트웨이는 데이터그램의 소스 포트 어드레스를 보조 넘버로 변환하고 소스 IP 어드레스를 게이트웨이의 외부 IP 어드레스로 변환한다. 그다음, 게이트웨이는 데이터그램이 ISAKMP 데이터그램과 합치하지 않기 때문에 타겟에 의해 거부되는 인터넷에 데이터그램을 전송한다. 이러한 동작은 도 7의 행 15, 16에 도시되어 있다.

도 3에서, 게이트웨이가 인터넷으로부터 수신된 데이터그램을 처리할 때 따르게 될 스텝을 아웃라인한 판정 차트가 도시되어 있다. 데이터그램의 수신시, 게이트웨이는 먼저 그 타입을 체크하고, 데이터그램이 암호화되었다면, SPI 가 그 내부 테이블내에 나타나 있는지를 보기 위해 체크한다. SPI가 인식되었다면, 그 행선 IP 어드레스는 로컬 디바이스의 IP 어드레스로 변환되고, 데이터그램은 로컬 디바이스로 전달되기 위해 LAN으로 전송된다. SPI가 인식되지 않았다면, 게이트웨이는 다음으로 데이터그램의 소스 어드레스에 상응하는 게이트웨이의 SPI-인 필드가 제로(0)인지를 보기 위하여 체크한다. SPI-인이 제로라면, 게이트웨이는 데이터그램이 새로운 세션의 제1 응답이라고 가정하고 SPI-인 필드내의 제로를 데이터그램의 SPI로 바꾼다. 게이트웨이는 행선 IP 어드레스를 LAN상의 디바이스의 로컬 IP 어드레스를 변환하고 데이터그램을 전달을 위해 LAN에 전송한다. 이러한 동작은 도 5b, 및 도 5c에 도시되어 있다. 도 5b에서, 로컬 머신 L-1에 대한 SPI-인은 제로로 셋정된다. 3288의 SPI를 갖는 인터넷으로부터 데이터그램을 게이트웨이가 수신할 때에, 게이트웨이는 SPI-인 필드내에 그 SPI를 찾지 못하게 된다. 게이트웨이는 다음으로, SPI-인 필드가 제로의 값을 유지하고 있는지를 보기 위하여 체크한다. 로컬 머신 L-1에 대한 SI-인이 제로라고 결정할 때, 게이트웨이는 제로를 데이터그램의 SPI('3288')로 바꾸고 LAN으로 이 데이터그램을 전송한다. 이것은 도 5c에 도시되어 있다.

도 3에서, 인터넷으로부터의 데이터그램이 암호화되지 않았다면, 게이트웨이는 그것이 500의 포트 어드레스를 가졌는지를 보기 위하여 체크한다. 데이터그램이 500의 포트 어드레스를 가지고 있지 않다면, 데이터그램은 외부 네트워크로부터 데이터그램에 대한 '정상' 어드레스 변환을 거치게 되는데, 이것은 LAN상의 디바이스의 로컬 포트 어드레스 및 로컬 IP 어드레스가 데이터그램의 행선 필드로 변경되고 데이터그램은 전달되기 위해 LAN에 전송되는 것을 의미한다. 인터넷으로부터의 데이터그램에 대한 이러한 '정상' 어드레스 변환은 도 6의 행 3, 4에 도시되어 있다.

다시 도 3에서, 데이터그램이 500의 포트 어드레스를 갖고 있지 않다면, 게이트웨이는 다음으로, 포트 500이 로컬 IP 어드레스에 바인드되어 데이터그램의 (외부) 소스 IP 어드레스와 관련되어 있는지를 보기 위해 체크해야 한다. 만약 그러하다면, 데이터그램은 유효하고, 행선 IP 어드레스가 외부 게이트웨이의 어드레스로부터 로컬 디바이스의 IP 어드레스로 변환된 후에 LAN으로 통과된다. LAN에 데이터그램을 통과시, 게이트웨이는 포트 500을 해제한다. 이러한 동작은 도 6의 행 7, 8에 도시되어 있다.

도 3에서, 포트 500이 로컬 IP 어드레스에 바인드되어 있고 데이터그램의 소스 IP 어드레스내에 발견된 것과 상이한 외부 I 어드레스와 관련되어 있다면, 데이터그램은 유효하지 않고 게이트웨이에 의해 더 이상 처리되지 않는다. 이러한 동작은 도 7의 행 25-31에 도시되어 있다. 행 25 및 행 26에서, 로컬 머신 L-1은 ISAKMP 데이터그램을 타겟 T-1에 전송한다. 이 포인트에서, 포트 500은 로컬 머신 L-1의 IP 어드레스에 바인드되고 타겟 T-1의 IP 어드레스와 관련되어 있다. 그러나, 도 7에 도시된 바와 같이, 타이머는 응답이 T-1로부터 게이트웨이에서 수신되기 전에 '타임' 아웃되고 행 27에서, 포트 500은 해제된다. 행 28,29에서, 로컬 머신 L-3은 ISAKMP 데이터그램을 타겟 T-3으로 전송하고, 포트 500을 L-3의 IP 어드레스로 바인드하고 T-3의 IP 어드레스와의 관련성을 생성한다. 포트 500이 바인드되면, 응답은 T-1로부터 수신된다. 그러나, 포트 500이 바인드되었기 때문에 T-3의 IP 어드레스와 관련되어 있고 T-1으로부터의 응답은 폐기된다. 이것은 도 7의 행 30, 31에 도시되어 있다.

도 5a-5c는 인터넷상의 타겟과 로컬 컴퓨터 사이의 암호화된 통신에 대한 SPI 넘버 및 IP 어드레스가 유지되는 게이트웨이의 내부 테이블을 도시하고 있다. 'L-1,' 'L-2,' 'L-x' 및 'T-1' 내지 'T-3'에 대한 필드는 참조의 용이를 위해 포함하되어 있고, 게이트웨이의 내부 테이블내에는 나타나지 않는다. 도 5에서, 필드 'SP-아웃'은 LAN 상의 특정 컴퓨터와의 보안 세션동안 각각의 타겟 머신에 대한 SPI를 홀딩한다. 'SPI-인' 필드는 로컬 컴퓨터에 대해 의도된 유효한 데이터그램을 의미하는 것으로 로컬 컴퓨터에 의해 인식될 상응하는 SPI를 준다. 도 5a는 시작 시간에서의 테이블을 도시한다. 8개의 로컬 컴퓨터는 테이블의 데이터의 수명 동안 3개의 타겟, T-1 내지 T-3로 암호화된 세션에 관련되어 있다. 이것은 각각의 로컬 머신이 그 IP 어드레스와 관련된 SPI-인을 도시한다는 사실에 의해 도시되어 있다. 오직 3개의 타겟만이 테이블내에 도시되어 있지만, 각각의 타겟이 각각의 로컬 머신과 통신하기 위해 상이한 SPI-아웃을 사용하고 있다는 것을 알 수 있다. 이러한 방식으로, 타겟은 어느 소스로부터 암호화된 데이터그램이 발생되었는지를 알게 된다.

도 5b는 도 5a와 동일한 로컬 및 타겟 컴퓨터를 도시한다. 그러나, 여기에서, L-1과 T-1 사이의 세션에 대한 SPI-아웃은 컴퓨터 사이의 새로운 세션을 나타내는 새로운 SPI이다. 새로운 세션이 일어나고 있다는 게이트웨이의 제1 표시는 테이블내에 없는 SPI-'14662'-를 갖는 LAN으로부터 암호화된 데이터그램을 게이트웨이가 수신하는 것이다. 게이트웨이는 데이터그램을 인터넷에 전송하지만, 또한 새로운 SPI를 상기 데이터그램에 대한 소스 및 행선 IP 어드레스와 관련된 SPI-아웃 필드내에 놓기 위하여 게이트웨이의 테이블을 수정한다. 게이트웨이는 새로운 SPI-인이 또한 예상된다는 것을 나타내기 위하여 마커로서 SPI-인 필드내에 제로를 놓는다. 도 5c는 새로운 SPI-'3288'-가 T-1로부터 수신된 데이터그램내에 포함되었다는 것을 도시한다. 이 SPI가 게이트웨이의 SPI-인 필드내에 입력되었다면 이러한 세션동안의 L-1과 T-1 사이의 추가 통신이 그것들의 메시지를 증명하기 위해 상기 SPI's를 사용하게 된다.

도 6은 인터넷상의 리모트 타겟과 통신하는 LAN 상의 단일 컴퓨터에 의해 본 발명의 게이트웨이를 통한 대표적인 데이터그램의 흐름의 차트이다. 이 차트의 각각의 행은 게이트웨이와의 LAN 인터페이스 또는 게이트웨이와의 인터넷 인터페이스중 어느 하나에서의 데이터그램내의 정보를 나타낸다. 연속 행은 일측으로부터 게이트웨이를 들어가서 타측에서 게이트웨이를 떠나는 데이터를 나타낸다. 게이트웨이는 LAN과

의 인터페이스에서 로컬 IP 어드레스이고 인터넷과의 인터페이스에서 글로벌 IP 어드레스일 수 있는 하나의 IP 어드레스를 갖는다. 도 6내의 행은 데이터그램이 통과하고 있는 게이트웨이의 측부, 데이터그램의 타입, 데이터그램의 소스 IP 어드레스 및 포트 어드레스, 데이터그램의 행선 IP 어드레스 및 포트 어드레스, 및 ESP 프로토콜을 사용하는 타입 50의 암호화된 데이터그램에 대한 데이터그램의 시큐어리티 파라미터 인덱스(SPI)를 나타낸다.

도 6이 행 1은 게이트웨이의 로컬 인터페이스에 도착하고 로컬 컴퓨터 L-1에 상응하는 소스 IP 어드레서와 인터넷상의 타겟 T-1 의 행선 IP 어드레스를 갖는 UDP 데이터그램을 나타낸다. 용이하게 읽을 수 있도록 도 4는 로컬 행선지 L-1 내지 L-3 및 타겟 행선지 T-1 내지 T-3과 상호 참조되는 IP 어드레스의 테이블을 제공한다. L-1에 대한 소스 포트 어드레스는 포트 6404이고, 타겟의 행선 포트는 포트 80이다. 데이터그램이 암호화되지 않았고 500의 포트 넘버를 나타내지 않기 때문에, 데이터그램은 '보조' 포트 어드레스, 포트 10425가 소스 포트 어드레스 필드로 바뀌고 게이트웨이의 외부 IP 어드레스가 데이터그램의 소스 IP 어드레스를 대신하게 되는 정상 변환을 거치게 된다. 변환된 소스 포트 어드레스가 '보조'로 불리지만, 이것은 게이트웨이에 의해 유지되는 예약되지 않고 현재 사용되지 않는 포트 어드레스의 풀로부터 취해진 시퀀스내에서 정상적으로 그 다음이 된다.

데이터그램이 게이트웨이를 나갈 때, 도 6의 행 2에 도시된 바와 같이, 게이트웨이의 어드레스 변환 펑션은 소스 IP 어드레스 대신에 데이터그램 헤더내에 게이트웨이의 외부 IP 어드레스스를 대입하고 소스 포트에 보조 넘버를 제공한다. 행 3,4는 타겟으로부터의 응답 데이터그램을 도시한다. 행 3에서, 타겟으로부터의 UDP 데이터그램은 행선 IP 어드레스를 게이트웨이의 외부 IP 어드레스로, 그리고 행선 포트를 게이트웨이에 의해 보조로 할당된 포트 어드레스로서 나타낸다. 데이터그램이 암호화되지 않고 500의 포트 어드레스를 갖고 있지 않기 때문에, 데이터그램은 행선 포트 어드레스 및 IP 어드레스의 정상 변환을 거친 후에 LAN으로 전송되게 된다. 행 4에서, 게이트웨이는 LAN으로 데이터그램을 전송하기 전에 헤더의 행선 필드내에 포트 어드레스 및 로컬 컴퓨터의 로컬 IP 어드레스를 대입한다.

도 6의 행 5에서, 로컬 컴퓨터는 타겟과의 ISAKMP 프로토콜을 초기화한다. 데이터 타입은 ISAKMP로서 표시되어 있다. 소스 및 행선 포트 어드레스는 포트 500이다. 행선 포트 어드레스가 포트 500이라고 게이트웨이가 결정할 때, 게이트웨이는 포트 500이 현재 임의의 IP 어드레스 바인드되었는지를 보기 위해 체크한다. 행선 포트 어드레스가 포트 500이 아니라면, 게이트웨이는 데이터그램을 통과시키고, 게이트웨이의 외부 IP 어드레스를 나타내기 위해 소스 IP 어드레스 필드만을 변환하지만, 소스 포트 어드레스를 변화시키지는 않는다.

도 5에서, 행 5 내지 16은 완전히 암호화되고 인증된 데이터그램을 지원하기 위해 SAs(시큐러티 어소시에이션)를 달성하는데 필요한 6개의 스탠더드 ISAKMP '핸드셰이킹' 데이터그램 교환을 나타낸다. ISAKMP의 일부 모델이 보다 적은 교환을 사용하지만, 메인 모드는 도 6에 묘사되어 있다. SAs의 달성에 이어, 로컬 컴퓨터 및 타겟은 ESP 프로토콜 암호화된 데이터그램을 사용하여 통신을 시작한다. 여기에서, 데이터그램 유효성은 데이터그램의 헤더의 SPI 필드내의 시큐어리티 파라미터 인덱싱(SPI)을 사용함으로써 유지된다. 각각의 호스트는 계속되는 시큐어리티를 보장하기 위해 필요한 대로 호스트의 상호 동의에 의해 세션 동안 수정될 수 있는 자체 SPI에 '어드레스'된 데이터그램을 인식한다. 암호화된 데이터그램이 도 6의 행 17 및 행 18에 나타낸 바와 같이 게이트웨이를 통과할 때, 데이터그램의 소스 IP 어드레스가 게이트웨이의 외부 IP 어드레스가 되도록 변환되지만, 소스와 행선 SPI 어떤 것도 게이트웨이에 의해 수정되지는 않는다.

따라서, 암호화된 데이터그램이 게이트웨이에 수신되었다면, 타입 50(ESP)의 데이터그램에 의해 표시된다. 그러한 데이터그램 타입을 만나게 되면, 게이트웨이는 SPI가 그 내부 테이블내에 레코드되었는지를 보기 위하여 데이터그램의 시큐어리티 파라미터 인덱스(SPI)를 체크한다. 만약, SPI가 그 내부 테이블에 레코드되었다면, 게이트웨이는 데이터그램의 소스 또는 행선 IP 어드레스를 적합한 것으로 변환하여 그 데이터그램을 전송 방향에 따라 LAN 또는 인터넷에 전송한다. 그러나, LAN으로부터의 데이터그램의 SPI가 게이트웨이의 내부 테이블에 나타나지 않고 소스 및 행선지가 IP 어드레스로 인식된다면 게이트웨이는 새로운 세션이 시작되었다고 인식하게 된다. 이러한 경우에, 게이트웨이는 새로운 SPI를 그대로 두는 외부 네트워크에 데이터그램을 보내지만, 게이트웨이의 내부 테이블의 'SPI-아웃' 필드내에 새로운 SPI를 레코드하고 제로를 'SPI-인'내에 놓게 된다. 행 25 및 26에서, 새로운 세션을 의미하는 새로운 SPI가 나타나는 것을 볼 수 있다. 이러한 이벤트는 'SPI-인' 필드내의 '0'가 '14662'의 새로운 SPI-아웃에 상응하는 도 5b에 상응한다. 행 27,28에서, 외부 네트워크로부터의 응답 패킷은 '이전' SPI '9802'가 '새로운' SPI '3288'로 교체되었음을 나타낸다.

도 7은 L-1, L-2, L-3으로 표시된 LAN상의 3개의 컴퓨터 사이의 데이터그램의 본 발명의 게이트를 통한 경로 및 유일한 글로벌 IP 어드레스를 갖는 인터넷상의 3개의 타겟, T-1, T-2, T-3을 설명하는 것을 제외하고는 도 6과 유사하다. 도 4에서, 용이한 참조를 위해 이러한 디바이스의 IP 어드레스를 포함하는 테이블이 주어져 있다. 도 7에 도시된 바와 같이, 'L-1 아웃'으로 표시된 전송은 로컬 컴퓨터(L-1)로부터 게이트웨이로의 전송을 나타낸다. 'T-1 인'은 게이트웨이로부터 타겟 T-1로의 전송을 나타낸다. 'T-1 아웃'은 타겟 T-1로부터 게이트웨이로의 전송을 나타내고, 'L-1 인'은 게이트웨이로부터 컴퓨터 L-1로의 전송을 나타낸다.

도 7의 행 1-8에 도시된 바와 같이, 컴퓨터 L-1 및 L-2는 타겟 T-1 및 T-2과 '클리어(in the clear)' 통신을 수행한다. 행 9에서, L-1은 T-1과 함께 ISAKMP 세션을 시작한다. 행 9-14는 ISAKMP 프로토콜 동안 L-1 및 T-1 사이에 교환되는 제1 3개의 메시지를 나타낸다. 행 15에서, 컴퓨터 L-3은 T-3과 함께 ISAKMP 메시지 교환을 시작한다. 그러나, 이 때에, 포트 500은 L-1에 바인드되고 T-1의 IP 어드레스와 관련되며, T-1으로부터 ISAKMP-4를 기다린다. 이러한 상황에서, L-3으로부터의 데이터그램은 포트 500을 바인드할 수 없고, 데이터그램의 소스 포트 어드레스는 변환된다. 이와 같이, L-3은 행 15에서 시작된 전송을 완료할 수 없다.

그후에, 행 17-18에서, T-1의 응답(ISAKMP-4)은 게이트웨이에서 수신되어 L-1로 전송되고, 포트 500이 즉시 유용하게 된다. 따라서, L-3이 그 ISAKMP-1 전송을 행 19에서 재시도할 때, 전송에 성공하게 된다.

도 7의 행 19-20에서, L-3의 ISAKMP-1 전송은 포트 500을 L-3의 IP 어드레스에 바인드한다. 따라서, L-1이 그 ISAKM-5 전송을 재시도할 때, 행 21-22에서, 포트 500은 유용하지 않고, 게이트웨이는 단순히 행선 포트 어드레스를 포트 500으로부터 '보조' 포트 넘버- 이경우에는 '9063'-로 변환하여, 타겟 T-1이 상기 데이터그램을 ISAKMP 데이터그램으로 인식하지 않는 인터넷으로 상기 데이터그램을 전송하게 된다. 그러나, L-3이 행 23-24에서 포트 500을 해제한 후에, L-1가 그 ISAKMP-5 전송을 보내려는 다음 시도는 T-1에 의해 성공적으로 수신되어진다. 그러나, T-1의 응답은 느리고, 행 27에서 포트 500은 그 바인딩으로부터 L-1로 해제되고, 행 28-29에서, ISAKMP-3 전송에 대하여 L-3에 의해 즉시 잡히게 된다. 따라서, T-1의 ISAKMP-6 응답이 게이트에 도착할 때, 행 30 및 31에 도시된 바와 같이, 포트 500은 차단되고, 데이터그램은 무시된다. 그후에, ISAKMP-5 메시지에 대한 응답을 수신하지 않은 L-1은 그 응답을 행 34-35에서 재전송하고, T-1로부터 응답이 행 36-37에서 수신된다. L-1 및 T-1은 그것들의 ISAKMP 핸드셰이킹에 이어 행 38-39 및 42-43에서 ESP 프로토콜을 사용하여 안전하게 통신할 수 있다.

도 7의 행 38-57은 다수의 로컬 컴퓨터 및 타겟 사이의 다양한 데이터그램을 게이트웨이가 처리하는 것을 보여준다. UDP 데이터그램은 행 40-41에 나타나 있고, ESP 데이터그램은 행 42-43 및 52-53에 나타나 있고, ISAMP 데이터그램은 행 44-45에 나타나 있다. 도 7의 차트가 각각의 디바이스에 대하여 상이한 IP 어드레스를 나타내지만, 실제로, 다수의 프로세스가 동일한 디바이스에서 실행되는 일이 일어날 수 있다. 게이트웨이에 의한 유일한 소스 포트의 대입, 암호화된 전송을 차별화하는 SPI's의 사용은 단일 머신에서 실행되는 다수의 프로세스로부터 나오는 데이터그램의 방향이 잘못 되지 않도록 보장한다.

도 8은 데이터그램 프로세싱 회로(100) 및 타이머(110) 사이의 신호의 초기화 및 전송을 도시한다. IP 어드레스로 바인드되는 포트 어드레스를 요구하는 이벤트가 발생할 때, 신호(120)는 타이밍을 시작하도록 타이머에 전송된다. 적합한 인터벌이 종료시에, 타이머는 타임이 종료되었다는 것을 나타내는 신호(140)를 전송하는데, 이러한 경우에 바인드되는 임의의 포트는 해제된다. 그 사이에, 예상된 데이터그램이 도착되고 이전에 바인드된 포트가 해제될 것이라면, 디스에이블링 신호(130)는 타이밍을 시작하기 위해 다음 신호를 기다리도록 타이머가 리셋되어야 한다는 것을 나타내는 타이머에 전송된다. 당업분야에 알려진 수많은 타이밍 회로가 존재하고 도 8에 도시된 특정 구성은 많은 가능한 실시예중 하나일 뿐이라는 것은 명백하다.

상술로부터, 여기에 설명된 바람직한 실시예만이 본 발명을 실현하는 수단이 아니고, 다른 실시예가 본 발명의 정신과 범위를 벗어남 없이 본 발명을 실현하기 위해 선택될 수 있다라는 것을 당업자는 이해할 것이다. 예를 들어, 바람직한 실시예가 ISAKMP 프로토콜과 사용하기 위해 배타적으로 예약된 포트 500에 관하여 설명하였지만, 본 발명은 추후 다른 프로세스 또는 프로토콜에 할당될 수 있는 다른 포트 어드레스가 행선지인 데이터그램을 처리하기 위해 동일한 방식으로 사용될 수 있다. 특별히, 인터넷에서 플레이되는 많은 게임은 정상적인 어드레스 변환을 견디어낼 없는 로컬 및 외부 머신상의 특정 포트의 사용을 필요로 한다. 또한, 본 발명이 사설 LAN 및 인터넷 사이의 통신에 대하여 주로 설명되었지만, 본 발명의 게이트웨이가 2개의 네트워크 사이의 임의의 인터페이스에서 사용될 수 있고 상술된 것과 동일한 기능을 가질 것이라는 것이 명백하다.

여기에 첨부된 청구항은 본 발명의 정신 및 범위내의 수정 및 변화를 포함하도록 의도되었다.

(57) 청구의 범위

청구항 1. LAN은 로컬 IP 어드레스를 사용하고, 게이트웨이는 상기 LAN상의 디바이스에 의해 보여질 수 있는 로컬 IP 어드레스 및 외부 네트워트상의 디바이스에 의해 보여질 수 있는 상기 외부 IP 어드레스를 가지며, 상기 LAN을 외부 네트워크에 연결하는 네트워크 어드레스 변환 게이트웨이에 있어서, 상기 게이트웨이는

상기 LAN 상의 로컬 디바이스의 로컬 IP 어드레스, 상기 외부 네트워크상의 외부 디바이스의 외부 IP 어드레스, SPI-인 값, SPI-아웃 값, 소스 포트 어드레스, 행선 포트 어드레스, 예약된 포트 어드레스의 조합을 관련시키고 예약된 포트 어드레스의 리스트를 유지하는 복수의 내부 테이블;

상기 LAN으로부터 상기 외부 네트워크로 전송되는 데이터그램 및 상기 외부 네트워크로부터 상기 LAN으로 전송되는 데이터그램에 대해 정상 어드레스 변환을 실행하는 수단;

상기 외부 네트워크상의 외부 디바이스에 전달하기로 의도된 데이터그램을 상기 LAN 상의 로컬 디바이스로부터 수신하고, 상기 데이터그램에 대한 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있는지를 결정하고, 상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있지 않다면, 상기 데이터그램에 대한 정상 어드레스 변환을 실행하고 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하고,

상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있다면, 상기 행선 포트 어드레스가 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드되었는지를 결정하고, 상기 행선 포트 어드레스가 상기 로컬 IP 어드레스에 바인드되어 있다면, 상기 데이터그램에 대한 정상 어드레스 변환을 실행하고 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하여

상기 행선 포트 어드레스가 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드되어 있지 않다면, 상기 데이터그램의 상기 소스 IP 어드레스를 상기 게이트웨이의 상기 외부 IP 어드레스가 되도록 수정하고, 상기 행선 포트 어드레스를 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드하고 상기 행선 포트 어드레스와 상기 외부 디바이스의 외부 IP 어드레스 사이에 연상을 생성하고, 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위하여 상기 외부 네트워크에 전송함으로써, 상기 LAN상의 로컬 디바이스로부터 상기 외부 네트워크상의 외부 디바이스로 상기 데이터그램을 전달하는 수단;을 포함하는 것을

특징으로 하는 네트워크 어드레스 변환 게이트웨이.

청구항 2. 제 1 항에 있어서, 상기 LAN상의 로컬 디바이스로부터 상기 외부 디바이스로 데이터그램을 전달하는 수단은, 상기 데이터그램이 암호화되었는지를 결정하고, 상기 데이터그램이 암호화되었다면, 상기 데이터그램의 SPI가 상기 내부 테이블내의 SPI-아웃 필드내에 레코드되어 있는지를 결정하고, 상기 SPI가 상기 SPI-아웃 필드내에 레코드되어 있다면, 상기 데이터그램의 소스 IP 어드레스를 상기 게이트웨이의 상기 외부 IP 어드레스가 되도록 수정하고 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하는 수단을 더 포함하는 것을 특징으로 하는 네트워크 어드레스 변환 게이트웨이.

청구항 3. 제 2 항에 있어서, 상기 SPI가 상기 내부 테이블의 상기 SPI-아웃 필드내에 레코드되어 있지 않다면, 상기 로컬 디바이스의 로컬 IP 어드레스에 상응하는 SPI-인 필드를 제로로 설정하고 상기 SPI-아웃 필드를 상기 SPI로 설정하며, 상기 데이터그램의 상기 소스 IP 어드레스를 상기 게이트웨이의 상기 외부 IP 어드레스가 되도록 수정하고 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하는 수단을 더 포함하는 것을 특징으로 하는 네트워크 어드레스 변환 게이트웨이.

청구항 4. 제 1 항에 있어서, 상기 네트워크 어드레스 변환 게이트웨이는, 상기 LAN상의 상기 로컬 디바이스로 전달되기로 의도된 데이터그램을 상기 외부 네트워크상의 상기 외부 디바이스로부터 수신함으로써 상기 외부 디바이스로부터 상기 로컬 디바이스로 데이터그램을 전달하고, 상기 데이터그램이 암호화되어 있는지를 결정하고, 상기 데이터그램이 암호화되어 있다면, 상기 데이터그램의 SPI가 상기 내부 테이블의 상기 SPI-인 필드내에 레코드되어 있는지를 결정하고, 상기 SPI가 상기 SPI-인 필드내에 레코드되어 있었다면, 상기 데이터그램의 행선 IP 어드레스를 상기 로컬 디바이스의 상기 로컬 IP 어드레스가 되도록 수정하고 상기 데이터그램을 상기 로컬 디바이스에 루팅 및 전달하기 위해 상기 LAN에 전송하고, 상기 SPI가 상기 내부 테이블의 상기 SPI-인 필드내에 레코드되어 있지 않다면, 상기 외부 디바이스의 상기 IP 어드레스에 상응하는 상기 SPI-인 필드가 제로인지를 결정하고, 상기 SPI-인 필드가 제로가 아니라면, 상기 데이터그램을 버리고, 상기 SPI-인 필드가 제로라면, 상기 SPI-인 필드를 상기 SPI와 동일하게 설정하고 상기 데이터그램의 행선 IP 어드레스를 상기 로컬 디바이스의 상기 로컬 IP 어드레스가 되도록 수정하고 상기 데이터그램을 상기 로컬 디바이스에 전달하기 위해 상기 LAN에 전송하고, 상기 데이터그램이 암호화되어 있지 않다면, 상기 데이터그램에 대한 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있는지를 결정하고, 상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있지 않다면, 상기 데이터그램에 대한 정상 어드레스 변환을 실행하고 상기 데이터그램을 상기 로컬 디바이스에 전달하기 위해 상기 LAN에 전송하고, 상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 상기 리스트내에 포함되어 있다면, 상기 행선 포트 어드레스가 상기 로컬 디바이스의 로컬 IP 어드레스에 바인드되어 있는지를 결정하고, 상기 행선 포트 어드레스가 상기 로컬 IP 어드레스에 바인드되어 있지 않다면, 상기 데이터그램을 버리고, 상기 행선 포트 어드레스가 상기 로컬 IP 어드레스에 바인드되어 있다면, 상기 데이터그램의 상기 행선 IP 어드레스를 상기 로컬 디바이스의 상기 로컬 IP 어드레스가 되도록 수정하고, 상기 로컬 IP 어드레스로부터 상기 행선 포트 어드레스를 바인드해제하고, 상기 데이터그램을 상기 로컬 디바이스에 전달기 위해 상기 LAN에 전송하는 수단을 더 포함하는 것을 특징으로 하는 네트워크 어드레스 변환 게이트웨이.

청구항 5. 제 1 항에 있어서, 타이머를 더 포함하고, 포트 어드레스가 IP 어드레스에 바인드되었다는 신호를 수신할 때, 상기 타이머는 소정의 시간 동안 타이밍을 시작하고, 상기 소정의 시간의 종료시에, 상기 포트 어드레스가 상기 IP 어드레스로부터 바인드해제되도록 하는 신호를 전송하고, 상기 포트 어드레스가 상기 소정의 시간의 종료전에 상기 IP 어드레스로부터 바인드해제되었다는 것을 나타내는 신호를 수신할 때, 상기 타이머는 타이밍을 중지하고 리셋되는 것을 특징으로 하는 네트워크 어드레스 변환 게이트웨이.

청구항 6. 제 1 항에 있어서, 상기 외부 네트워크는 인터넷인 것을 특징으로 하는 네트워크 어드레스 변환 게이트웨이.

청구항 7. 제 6 항에 있어서, 상기 LAN은 가상 사설망인 것을 특징으로 하는 네트워크 어드레스 변환 게이트웨이.

청구항 8. 로컬 IP 어드레스를 사용하는 LAN상의 로컬 디바이스로부터 네트워크 변환 게이트웨이를 통하여 외부 네트워크상의 외부 디바이스로 IP 데이터그램을 처리하는 방법에 있어서,

상기 LAN상의 로컬 디바이스의 로컬 IP 어드레스, 상기 외부 네트워크상의 외부 디바이스의 외부 IP 어드레스, 상기 로컬 디바이스의 포트 어드레스, 상기 외부 디바이스의 포트 어드레스, SPI-인 값, SPI-아웃 값, 및 예약된 포트 어드레스, 및 예약된 포트 어드레스의 리스트를 관련시키는 복수의 테이블을 유지하는 단계;

상기 LAN으로부터 데이터그램을 수신하는 단계;

상기 데이터그램에 대한 행선 포트 어드레스가 상기 예약된 포트 어드레스의 테이블내에 포함되어 있는지를 결정하고, 상기 행선 포트 어드레스가 상기 예약된 포트 어드레스내에 포함되어 있지 않다면, 상기 데이터그램에 대한 정상 어드레스 변환을 실행하고 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하는 단계;

상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 테이블내에 포함되어 있다면, 상기 행선 포트 어드레스가 IP 어드레스에 바인드되어 있는지를 결정하고, 상기 행선 포트 어드레스가 IP 어드레스에 바인드되어 있다면, 상기 데이터그램에 대한 정상 어드레스 변환을 실행하고 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하는 단계;

상기 행선 포트 어드레스가 IP 어드레스에 바인되어 있지 않다면, 상기 소스 IP 어드레스를 상기 외부 디바이스에 대한 상기 외부 IP 어드레스가 되도록 수정하고, 상기 행선 포트 어드레스를 상기 로컬 디바이스의 로컬 IP 어드레스에 바인드하고 상기 행선 포트 어드레스와 상기 외부 디바이스의 상기 외부 IP 어

드레스 사이의 연상을 생성하고, 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하는 단계;를 포함하는 것을 특징으로 하는 방법.

청구항 9. 제 8 항에 있어서,

상기 데이터그램이 암호화되어 있는지를 결정하고, 상기 데이터그램이 암호화되어 있다면, 상기 데이터그램내의 SPI가 상기 복수의 인터넷 테이블중 하나의 SPI-아웃내에 레코드되어 있는지를 결정하고, 상기 SPI가 상기 인터넷 테이블의 상기 SPI-아웃 필드내에 레코드되어 있다면, 상기 소스 IP 어드레스를 상기 게이트웨이의 외부 IP 어드레스가 되도록 수정하고 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하고, 상기 SPI가 상기 내부 테이블의 상기 SPI-아웃 필드내에 레코드되어 있지 않다면, 상기 외부 디바이스의 IP 어드레스에 상응하는 상기 SPI-아웃 필드를 상기 SPI와 동일하게 설정하고 상기 내부 테이블의 SPI-인 필드를 제로로 설정하고, 상기 소스 IP 어드레스를 상기 게이트웨이의 상기 외부 IP 어드레스가 되도록 수정하고, 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 데이터그램을 상기 외부 네트워크에 전송하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 10. 외부 네트워크상의 외부 디바이스로부터 네트워크 변환 게이트웨이를 통하여 로컬 IP 어드레스를 사용하는 LAN상의 로컬 디바이스로 IP 데이터그램을 처리하는 방법에 있어서,

상기 LAN상의 로컬 디바이스의 로컬 IP 어드레스, 상기 외부 네트워크상의 외부 디바이스의 외부 IP 어드레스, 상기 로컬 디바이스의 포트 어드레스, 상기 외부 디바이스의 포트 어드레스, SPI-인 값, SPI-아웃 값, 및 예약된 포트 어드레스, 및 예약된 포트 어드레스의 리스트를 관련시키는 복수의 테이블을 유지하는 단계;

데이터그램을 상기 외부 네트워크로부터 수신하는 단계;

상기 데이터그램이 암호화되어 있는지를 결정하고 상기 데이터그램이 암호화되어 있지 않다면, 상기 데이터그램에 대한 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있는지를 결정하고, 상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있지 않다면, 정상 어드레스 변환을 실행하여 상기 데이터그램을 상기 로컬 디바이스에 루팅 및 전달하기 위해 상기 LAN에 전송하는 단계;

상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있다면, 상기 포트 어드레스가 상기 로컬 IP 어드레스에 바인드되어 있는지를 결정하고, 상기 행선 포트 어드레스가 상기 로컬 IP 어드레스에 바인드되어 있지 않다면, 상기 데이터그램을 버리는 단계;

상기 행선 포트 어드레스가 상기 로컬 IP 어드레스에 바인드되어 있다면, 상기 행선 IP 어드레스를 상기 로컬 디바이스의 상기 로컬 IP 어드레스가 되도록 수정하고, 상기 행선 포트 어드레스를 상기 로컬 IP 어드레스로부터 바인드해제하고, 상기 데이터그램을 상기 로컬 디바이스에 루팅 및 전달하기 위해 상기 LAN에 전송하는 단계;를 포함하는 것을 특징으로 하는 방법.

청구항 11. 제 10 항에 있어서, 상기 방법은 상기 데이터그램이 암호화되어 있다면,

상기 데이터그램내의 SPI가 상기 복수의 내부 테이블중 하나의 SPI-인 필드내에 레코드되어 있는지를 결정하고, 상기 SPI가 상기 내부 테이블의 상기 SPI-인 필드내에 레코드되어 있다면, 행선 IP 어드레스가 상기 로컬 디바이스의 내부 IP 어드레스가 되도록 수정하고 상기 데이터그램을 상기 로컬 디바이스에 루팅 및 전달하기 위해 상기 LAN에 전송하는 단계;

상기 SPI가 상기 내부 테이블의 상기 SI-인 필드내에 레코드되어 있지 않다면, 상기 외부 디바이스의 IP 어드레스에 상응하는 상기 SPI-인 필드가 제로인지를 결정하고, 상기 SPI-인 필드가 제로가 아니라면, 상기 데이터그램을 버리는 단계;

상기 SPI -인 필드가 제로라면, 상기 SPI인 필드를 상기 SPI가 되도록 수정하고, 상기 행선 IP 어드레스를 상기 로컬 디바이스의 상기 로컬 IP 어드레스가 되도록 수정하고, 상기 데이터그램을 상기 로컬 디바이스에 루팅 및 전달하기 위해 상기 LAN에 전송하는 단계;를 더 포함하는 것을 특징으로 하는 방법.

청구항 12. 제 11 항에 있어서,

상기 행선 포트 어드레스가 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드될 때마다 타이머를 시작하는 단계;

상기 행선 포트 어드레스가 해제될 때마다 상기 타이머를 리셋하는 단계; 및

상기 타이머가 액티브하고 상기 타이머가 시작된 시점으로부터 소정의 시간이 종료될 때마다 신호를 전송하는 단계;를 더 포함하는 것을 특징으로 하는 방법.

청구항 13. 제 12 항에 있어서, 상기 포트 어드레스가 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드될 때마다 타이머를 시작하는 단계;

상기 행선 포트 어드레스가 해제될 때마다 상기 타이머를 리셋하는 단계;

상기 타이머가 액티브하고 상기 타이머가 시작된 시점으로부터 소정의 시간이 종료될 때마다 신호를 전송하는 단계;를 더 포함하는 것을 특징으로 하는 방법.

청구항 14. 제 11 항에 있어서, 상기 외부 네트워크는 인터넷인 것을 특징으로 하는 방법.

청구항 15. 제 12 항에 있어서, 상기 외부 네트워크는 인터넷인 것을 특징으로 하는 방법.

청구항 16. 제 11 항에 있어서, 상기 LAN은 가상 사설망인 것을 특징으로 하는 방법.

청구항 17. 제 12 항에 있어서, 상기 LAN은 가상 사설망인 것을 특징으로 하는 방법.

청구항 18. LAN을 네트워크 어드레스 변환 게이트웨이를 통해 외부 네트워크에 연결하고 머신에 의해 실행가능한 복수의 코드 섹션을 갖는 컴퓨터 프로그램을 저장한 머신 판독가능 기억장치에 있어서, 상기 LAN상의 디바이스에 의해 보여질 수 있는 로컬 IP 어드레스를 갖고 상기 외부 네트워크상의 디바이스에 의해 보여질 수 있는 외부 IP 어드레스를 가지며, 상기 LAN상의 로컬 디바이스의 로컬 IP 어드레스, 상기 외부 네트워크상의 외부 디바이스의 외부 IP 어드레스, 소스 포트 어드레스, 행선 포트 어드레스, 예약된 포트 어드레스, 및 예악된 포트 어드레스의 리스트의 조합을 관련시키는 복수의 내부 테이블을 더 포함하는 상기 게이트웨이는 상기 머신이

상기 외부 네트워크상의 외부 디바이스에 전달하기로 의도된 데이터그램을 상기 LAN 상의 로컬 디바이스로부터 수신함으로써 상기 LAN상의 로컬 디바이스로부터 상기 외부 네트워크상의 외부 디바이스에 데이터그램을 전달 시도하는 단계;

상기 데이터그램에 대한 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있는지를 결정하고 상기 행선 포트 어드레스가 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드되어 있는지를 결정하는 단계;

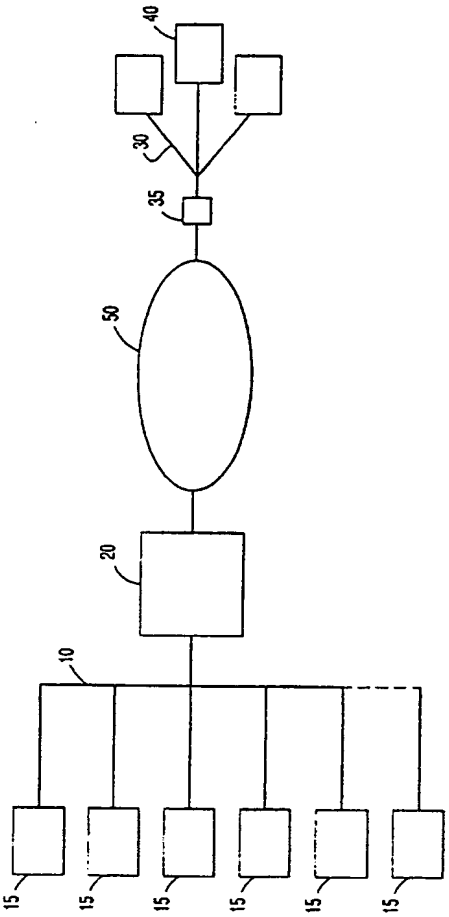
상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있지 않다면 상기 데이터그램에 대해 정상 어드레스 변환을 실행하고 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 상기 데이터그램을 전송하는 단계;

상기 행선 포트 어드레스가 상기 예약된 포트 어드레스의 리스트내에 포함되어 있고 상기 행선 포트 어드레스가 상기 로컬 IP 어드레스에 바인드되어 있다면, 상기 데이터그램에 대한 정상 어드레스 변환을 실행하고 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 상기 데이터그램을 전송하는 단계; 및

상기 데이터그램의 상기 소스 IP 어드레스를 상기 게이트웨이의 상기 외부 P 어드레스가 되도록 수정하고, 상기 행선 포트 어드레스를 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드하고 상기 행선 포트 어드레스와 상기 외부 디바이스의 외부 IP 어드레스 사이의 연상을 생성하며, 상기 행선 포트 어드레스가 상기 로컬 디바이스의 상기 로컬 IP 어드레스에 바인드되어 있지 않다면 상기 데이터그램을 상기 외부 디바이스에 루팅 및 전달하기 위해 상기 외부 네트워크에 전송하는 단계;를 실행하도록 돕는 것을 특징으로 하는 머신 판독가능 기억장치.

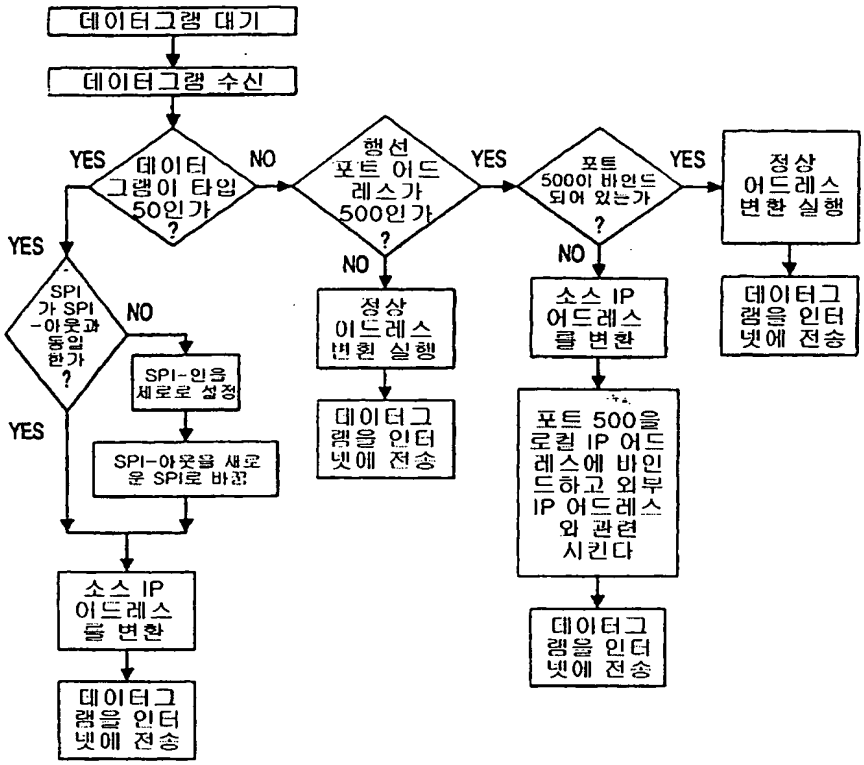
도면

도면1



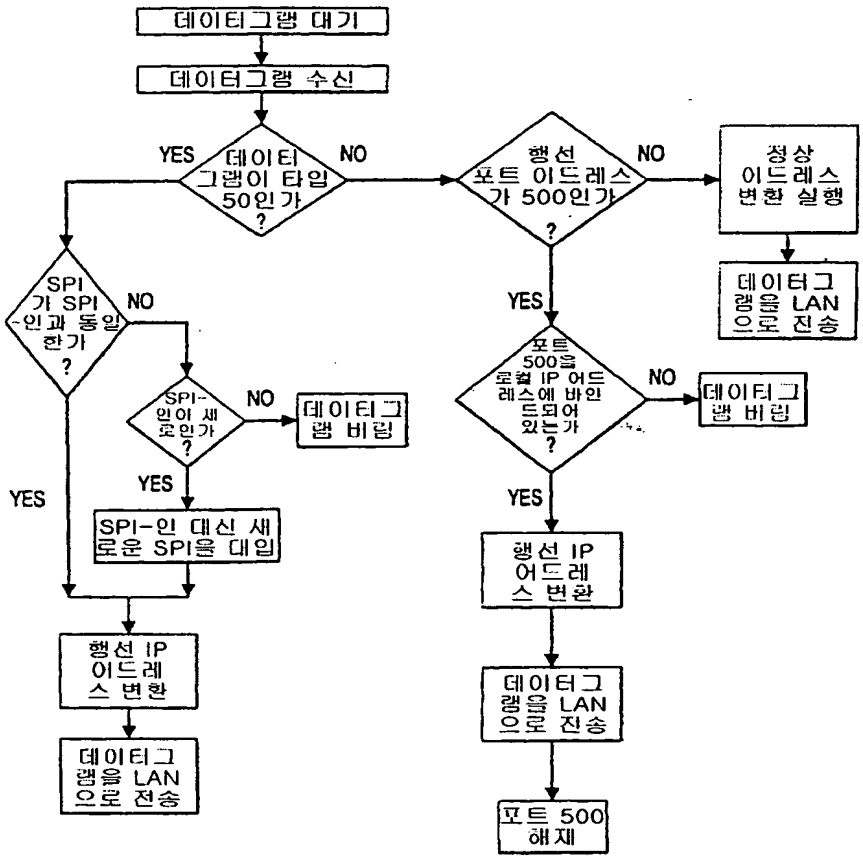
도면2

LAN으로부터의 데이터그램에 대한 판정 트리



도면3

인터넷으로부터의 데이터그램에 대한 판정 트리



도면4

ID 어드레스				
	로컬 컴퓨터	게이트웨이 내부	게이트웨이 외부	타겟
L-1	192.168.0.2	102.168.0.1	142.140.3.6	204.71.202.160 T-1
L-2	192.168.0.4	102.168.0.1	142.140.3.6	207.46.131.137 T-2
L-3	192.168.0.3	102.168.0.1	142.140.3.6	207.158.227.235 T-3

도면5a

SPI 테이블-3개의 호스트와 통신하는 8개의 로컬 컴퓨터				
	타겟	로컬 IP	SPI-아웃	SPI-인
T-1	204.71.202.160	192.168.0.2 L-1	4859	9802
		192.168.0.5 L-X	52856	7000
		192.168.0.10 L-X	8565	8523
T-2	207.46.131.137	192.168.0.4 L-2	1353	6234
		192.168.0.7 L-X	2562	10125
		192.168.0.10 L-X	25763	12106
T-3	207.158.227.235	192.168.0.3 L-3	38935	7753
		192.168.0.8 L-X	9093	32828

도면5b

새로운 세션 - 새로운 SPI-아웃 - 0으로 설정된 SPI-인				
	타겟	로컬 IP	SPI-아웃	SPI-인
T-1	204.71.202.160	192.168.0.2 L-1	14662	0
		192.168.0.5 L-X	52856	7000
		192.168.0.10 L-X	8565	8523
T-2	207.46.131.137	192.168.0.4 L-2	1353	4562
		192.168.0.7 L-X	2562	10125
		192.168.0.10 L-X	25763	12106
T-3	207.158.227.235	192.168.0.3 L-3	8773	20889
		192.168.0.8 L-X	9093	32828

도면5c

수신된 응답 패킷 - 수신된 새로운 SPI-인				
	타겟	로컬 IP	SPI-아웃	SPI-인
T-1	207.200.0.2	192.168.0.2 L-1	14662	3288
		192.168.0.5 L-X	52856	7000
		192.168.0.10 L-X	8565	8523
T-2	206.23.5.120	192.168.0.4 L-2	1353	6234
		192.168.0.7 L-X	43966	17937
		192.168.0.10 L-X	25763	12106
T-3	207.198.75.3	192.168.0.3 L-3	8773	20889
		192.168.0.8 L-X	9093	32828

도면6a

게이트웨이를 통하는 패킷의 시퀀스
단일 로컬 머신 -- 단일 타겟

경로	데이터그램 타입	소스 어드레스 IP	소스 어드레스 포트	행선 어드레스 IP	행선 어드레스 포트	SPI	행
LAN - GATE	UDP	192.168.0.2	6404	204.71.202.160	80		1
GATE - NET	UDP	142.140.3.6	10425	204.71.202.160	80		2
NET - GATE	UDP	204.71.202.160	80	142.140.3.6	10425		3
GATE - LAN	UDP	204.71.202.160	80	192.168.0.2	6404		4
LAN - GATE	ISAKMP-1	192.168.0.2	500	204.71.202.160	500		5
GATE - NET	ISAKMP-1	142.140.3.6	500	204.71.202.160	500		6
NET - GATE	ISAKMP-2	204.71.202.160	500	142.140.3.6	500		7
GATE - LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500		8
LAN - GATE	ISAKMP-3	192.168.0.2	500	204.71.202.160	500		9
GATE - NET	ISAKMP-3	142.140.3.6	500	204.71.202.160	500		10
NET - GATE	ISAKMP-4	204.71.202.160	500	142.140.3.6	500		11
GATE - LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500		12
LAN - GATE	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		13
GATE - NET	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		14
NET - GATE	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		15
GATE - LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500		16

도면6b

LAN-GATE	ESP (50)	192.168.0.2	204.71.202.160	4859	17
GATE-NET	ESP (50)	142.140.3.6	204.71.202.160	4859	18
NET-GATE	ESP (50)	204.71.202.160	142.140.3.6	9802	19
GATE-LAN	ESP (50)	204.71.202.160	192.168.0.2	9802	20
LAN-GATE	ESP (50)	192.168.0.2	204.71.202.160	4859	21
GATE-NET	ESP (50)	142.140.3.6	204.71.202.160	4859	22
NET-GATE	ESP (50)	204.71.202.160	142.140.3.6	9802	23
GATE-LAN	ESP (50)	204.71.202.160	192.168.0.2	9802	24
LAN-GATE	ESP (50)	192.168.0.2	204.71.202.160	14662	25
GATE-NET	ESP (50)	142.140.3.6	204.71.202.160	14662	26
NET-GATE	ESP (50)	204.71.202.160	142.140.3.6	3288	27
GATE-LAN	ESP (50)	204.71.202.160	192.168.0.2	3288	28
LAN-GATE	ESP (50)	192.168.0.2	204.71.202.160	14662	29
GATE-NET	ESP (50)	142.140.3.6	204.71.202.160	14662	30
NET-GATE	ESP (50)	204.71.202.160	142.140.3.6	3288	31
GATE-LAN	ESP (50)	204.71.202.160	192.168.0.2	3288	32

도면7a

게이트웨이를 통하는 패킷의 시퀀스
다수의 로컬 머신 -- 다수의 타겟

경로	패킷 타입	소스 어드레스 IP	소스 어드레스 서비스	행선 어드레스 IP	행선 어드레스 서비스	SPI	액티브 프로세스	행
LAN-GATE	UDP	192.168.0.2	6404	204.71.202.160	80		L:1 OUT	1
GATE-NET	UDP	142.140.3.6	10425	204.71.202.160	80		T:1 IN	2
LAN-GATE	UDP	192.168.0.4	4562	207.46.131.137	1353		L:2 OUT	3
GATE-NET	UDP	142.140.3.6	37525	207.46.131.137	1353		T:2 IN	4
NET-GATE	UDP	204.71.202.160	80	142.140.3.6	10425		T:1 OUT	5
GATE-LAN	UDP	204.71.202.160	80	192.168.0.2	6404		L:1 IN	6
NET-GATE	UDP	207.46.131.137	1353	142.140.3.6	37525		T:2 OUT	7
GATE-LAN	UDP	207.46.131.137	1353	192.168.0.4	4562		L:2 IN	8
LAN-GATE	ISAKMP-1	192.168.0.2	500	204.71.202.160	500		L:1 OUT-192.168.0.에 포트 500 바인드	9
GATE-NET	ISAKMP-1	142.140.3.6	500	204.71.202.160	500		T:1 IN-204.71.202.160과 관련	10
NET-GATE	ISAKMP-2	204.71.202.160	500	142.140.3.6	500		T:1 OUT	11
GATE-LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500		L:1 IN-포트 500 해제	12
LAN-GATE	ISAKMP-3	192.168.0.2	500	204.71.202.160	500		L:1 OUT-192.168.0.에 포트 500 바인드	13
GATE-NET	ISAKMP-3	142.140.3.6	500	204.71.202.160	500		T:1 IN-204.71.202.160과 관련	14
LAN-GATE	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L:3 OUT	15
GATE-NET	ISAKMP-1	142.140.3.6	500	207.158.227.235	8773		T:3 IN-포트 500 사용불능	16

도면7b

NET-GATE	ISAKMP-4	204.71.202.160	500	142.140.3.6	500		T-1 OUT	17
GATE-LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500		L-1 IN-포트 500 해제	18
LAN-GATE	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L-3 OUT	19
GATE-NET	ISAKMP-1	142.140.3.6	500	207.158.227.235	500		T-3 IN-192.168.0.3에 포트 500 바인드	20
LAN-GATE	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 OUT-포트 500 사용불능	21
GATE-NET	ISAKMP-5	142.140.3.6	500	204.71.202.160	9063		T-1 IN-소스 포트 이드레스 빈칸	22
NET-GATE	ISAKMP-2	207.158.227.235	500	142.140.3.6	500		T-3 OUT	23
GATE-LAN	ISAKMP-2	207.158.227.235	500	192.168.0.3	500		L-3 IN-포트 500 해제	24
LAN-GATE	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 OUT-192.168.0.0에 포트 500 바인드	25
GATE-NET	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 IN-204.71.202.160과 관련	26
							TIME-OUT FOR T-1 OUT-포트 500 해제	27
LAN-GATE	ISAKMP-3	192.168.0.3	500	207.158.227.235	500		L-3 OUT	28
GATE-NET	ISAKMP-3	142.140.6.3	500	207.158.227.235	500		T-3 IN-192.168.0.3에 포트 500 바인드	29
NET-GATE	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 OUT-포트 500 차단	30
							T-1 OUT-패킷 무시	31
NET-GATE	ISAKMP-4	207.158.227.235	500	142.140.3.6	500		T-3 OUT	32
GATE-LAN	ISAKMP-4	207.158.227.235	500	192.168.0.3	500		L-3 IN-포트 500 해제	33
LAN-GATE	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 OUT-192.168.0.0에 포트 500 바인드	34
GATE-NET	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 IN-204.71.202.160과 관련	35
NET-GATE	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 OUT	36
GATE-LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500		L-1 IN-포트 500 해제	37
LAN-GATE	ESP (50)	192.168.0.2		204.71.202.160		4859	L-1 OUT	38
GATE-NET	ESP (50)	142.140.3.6		204.71.202.160		4859	T-1 IN	39

도면7c

LAN-GATE	UDP	192.168.0.4	4562	207.46.131.137	1353		L-2 OUT	...	40
GATE-NET	UDP	142.140.3.6	37525	207.46.131.137	1353		T-2 IN		41
NET-GATE	ESP (50)	204.71.202.160		142.140.3.6		9802	T-1 OUT		42
GATE-LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	L-1 IN		43
LAN-GATE	ISAKMP-5	192.168.0.3	500	207.158.227.235	500		L-3 OUT	192.168.0.3에 포트 500 바인드	44
GATE-NET	ISAKMP-5	142.140.6.3	500	207.158.227.235	500		T-3 IN - 207.158.227.23과 관련		45
LAN-GATE	ESP (50)	192.168.0.2		204.71.202.160		4859	L-1 OUT		46
GATE-NET	ESP (50)	142.140.3.6		204.71.202.160		4859	T-1 IN		47
NET-GATE	ISAKMP-6	207.158.227.235	500	142.140.3.6	500		T-3 OUT		48
GATE-LAN	ISAKMP-6	207.158.227.235	500	192.168.0.3	500		L-3 IN - 포트 500 해제		49
NET-GATE	UDP	207.46.131.137	1353	142.140.3.6	37525		T-2 OUT		50
GATE-LAN	UDP	207.46.131.137	1353	192.168.0.4	4562		L-2 IN		51
LAN-GATE	ESP (50)	192.168.0.3		207.158.227.235		38935	L-3 OUT		52
GATE-NET	ESP (50)	142.140.6.3		207.158.227.235		38935	T-3 IN		53
NET-GATE	ESP (50)	204.71.202.160		142.140.3.6		9802	T-1 OUT		54
GATE-LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	L-1 IN		55
NET-GATE	ESP (50)	207.158.227.235		142.140.3.6		7753	T-3 OUT		56
GATE-LAN	ESP (50)	207.158.227.235		192.168.0.3		7753	L-3 IN		57

도면8